Chapter 8

[P2] Known- plaintext attack
→ 7- letters known
→ For all un-Known possible 26!
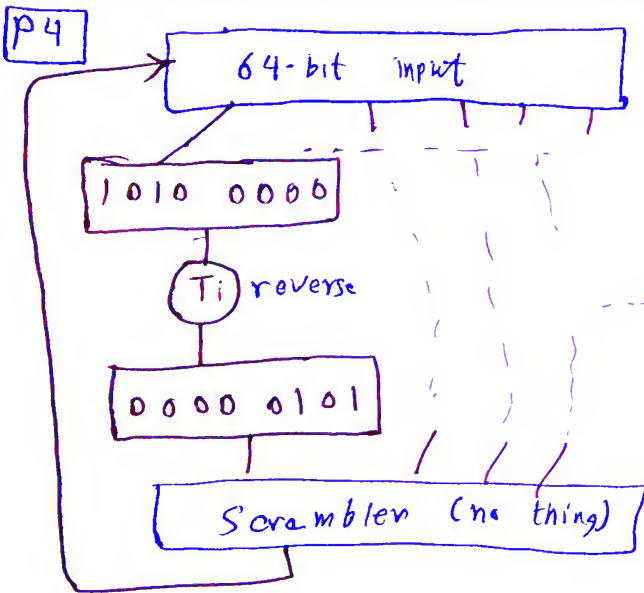→ frm 7 letters known

$$(26-7)! = 19!$$

We reduce possiblty by

$$26! - 19! = 10^9$$

[P3] Yes, It's possible to know the key of cipher 1,2 ((shift))

[P4]

(a) result after n=3
[0 0 0 0 0 1 0 1][0 0 0 0 0 1 0 1]----

(b) the input
[1 0 1 0 0 0 0 0]---- 1 0 1 0 0 0 0!
the result
[0 0 0 0 0 1 0 1]--- 1 0 0 0 0 1 0 1

(c) Scrambler also reverse order

ميي بييء القوسير الى
هو الجزء المتكرر

Step 1
before Scrambler
[0 0 0 0 0 1 0 1]----- 1 0 0 0 0 1 0 1
after
1 0 1 0 0 0 0 1 ---[1 0 1 0 0 0 0 0]

Step 2
before Scrambler
1 0 0 0 0 1 0 1 --- [0 0 0 0 0 1 0 1]
after
[1 0 1 0 0 0 0 0]--- 1 0 1 0 0 0 0 1

Step 3
before
[0 0 0 0 0 1 0 1}--- 1 0 0 0 0 1 0 1
after
1 0 1 0 0 0 0 1 --- [1 0 1 0 0 0 0 0]

[P6] (a) 1 0 0   1 0 0   1 0 0
         0 1 1   0 1 1   0 1 1

(b) She can know the pattern

(c) m(1) = 100
    m(2) = 100
    m(3) = 100

→ IV = c(0) = 111

→ C(1) = K_s(c(0) ⊕ m(1))
       = K_s(011) = 100

→ C(2) = K_s (c(1) ⊕ m(2))
       = K_s (000) = 110

→ C(3) = K_s (c(2) ⊕ m(3))
       = K_s (010) = 101

m = 100 100 100   C = 100 110 101

[P7] P = 3   q = 11

① n = P·q = 33

②
z = (P-1)(q-1) = 20

e < n   e → has no comma factor
with z

20 → 20 10 5 4 2

e = 9 → we choose this

$e * \underline{d} \ \%z \ = 1$

d = ??

$9 * d \ \% 20 = 1$

$9 * 9 \ \% 20 = 1$

d = 9

③ $C = m^e \ \%n$

'd' → m = 4 → $C = 4^9 \%33$

'o' → m = 15 → $C = 15^9 \%33$

'g' → m = 7 → $c = 7^9 \%33$

④ $m = c^d \ \%n$

[P9] $T_A = 9^{S_A} \ \%P$

$T_B = \dfrac{9^{S_B} \ \%P}{}$

$S = T_B^{S_A} \ \%P$ ⎤
⎥ → Prove
$S' = T_A^{S_B} \ \%P$ ⎦ that
they
are
equal

$S = [\ 9^{S_B} \ \%P\ ]^{S_A} \%P$) → المعادلة في برهان

$= 9^{S_A S_B} \ \% P$

$= [\ 9^{S_A} \ \%P\ ]^{S_B} \ \%P$

$= T_A^{S_B} \ \%P \ = S'$